Innovationen und enthaftende Wirkung eines Product- oder Nachhaltigkeits-Compliance-Managementsystems im Lichte aktueller höchstrichterlicher Rechtsprechung

Josef Scherer*

Innovationen wie neue Technologien, Produkte oder sonstige Leistungen mit noch unbekannten Auswirkungen werden in vielen Organisationen/Unternehmen oft ohne Kenntnis der negativen (technischen, rechtlichen und wirtschaftlichen) Auswirkungen unstrukturiert entwickelt oder eingesetzt: Nicht nur der verstärkte Einsatz von KI, sondern auch nicht abschließend bekannte chemische, physikalische oder sonstige Wirkungen von Produkten und Leistungen bergen existenzielle Gefahren in der Zukunft. Die Verletzung von Rechtsgütern wie Leib und Leben, Intellectual Property (IP) und Umweltstrafrechts-, Informationssicherheits-, Datenschutz-, Geschäftsgeheimnis-, Governance-Regularien u.v.m. sind an der Tagesordnung:
Die Haftungsverantwortung hierfür tragen primär und letztlich das Leitungs- (Vorstand, Geschäftsführer) und Aufsichtsgremium (Aufsichtsrat/Beirat). Gesetze, Rechtsprechung, verbindliche Regelungen der Exekutive, Stand der Technik, Standards, interne verbindliche Vorgaben (Richtlinien/Policies, Betriebsvereinbarungen, etc.) u.v.m. bilden den z.T. haftungsbewehrten Compliance-Rahmen, den häufig noch niemand so richtig erkannt hat – ebenso wie die Gefahren von Innovationen, die den Chancen risikobasiert und nach den Vorgaben der Business Judgment Rule gegenübergestellt werden müssen (§ 93 Abs. 1 Satz 2 AktG). Hier besteht noch großer Aufklärungsbedarf. Ein Compliance-Managementsystem kann enthaftend wirken und eine produktive Geschäftstätigkeit unter Nutzung der Chancen der Innovation ermöglichen. Der folgende Beitrag legt dar, dass Product- oder Nachhaltigkeits-Compliance-Management integraler Bestandteil des allgemeinen Compliance-Managementsystems und Teil der Governance, also des verbindenden „G" bei ESG und GRC, ist und inzwischen auch gesondert auditiert und zertifiziert werden kann.

I. Einführung

Ende Januar 2024 wurde ein deutscher Pharmakonzern im Zusammenhang mit angeblich schädlichen Wirkungen seines Produktes (Herbizd) durch ein Gericht in Philadelphia in einem einzigen Fall zu einer Zahlung von Strafschadensersatz („Punitive Damage) in Höhe von 2,25 Milliarden Dollar an einen krebskranken Mann verurteilt. Diese Schadensersatzart, die dem deutschen Recht fremd ist, wird in den USA und Kanada bei besonderer Verwerflichkeit und Rücksichtslosigkeit von einer Geschworenen-Jury festgesetzt. Der Verlust des Wertes des Konzerns an der Börse seit Involvierung in die zahlreichen Produkthaftungsfälle im Zusammenhang mit dem Herbizid, über dessen schädliche Wirkung die Wissenschaftler noch immer streiten, mag ein Vielfaches der Schadensersatzsumme betragen. Der Konzern will gegen das Urteil in Berufung gehen.

Sowohl nach den US Sentencing Guidelines, aber auch nach neuester höchstrichterlicher europäischer und deutscher Rechtsprechung kann ein Compliance-Managementsystem den Vorwurf vorsätzlichen oder sorglosen Verhaltens widerlegen.

Ebenso Ende Januar 2024 wurden Bergbaukonzerne in Brasilien verurteilt. Fast 9 Milliarden EUR müssen die Konzerne für die Verletzung von Menschenrechten aufgrund einer Umweltkatastrophe durch einen Dammbruch bezahlen.

Produkthaftungsfälle können – gerade im Mittelstand – existenzbedrohend sein. Egal, welche Innovationen, Produkte, Leistungen zu erfinden, bewerten, regulieren und zu steuern sind, der rechtliche Rahmen dafür ist „Technical Governance",[1] auf Basis von Compliance-, Risiko- und neuerdings auch Nachhaltigkeits-Management.

II. First steps für „Angemessenheit" und „Wirksamkeit" eines (Innovational Product oder Nachhaltigkeits-)Compliance-Managementsystems

1. Achtsamkeit, Bildung und Kommunikation

Zunächst sind ein allgemeines Verständnis bzgl. der naturwissenschaftlichen, technischen, rechtlichen, wirtschaftlichen und verhaltensökonomischen Implikationen der Innovation sowie entsprechende Kultur (Tone from the Top), Kompetenzen und Bewusstsein durch Schulungen und sonstige Kommunikations- und Achtsamkeits-Kampagnen zu schaffen.

2. Innovational Product oder Nachhaltigkeits-Compliance-Anforderungen und Compliance-Risiko-Analyse

Die Geschäftsleitung und sonstige Verantwortliche müssen parallel dazu primär die jeweiligen von ihnen betreuten (Prozess-)Themenfelder/Bereiche an aktuellen Anforderungen aus Gesetzgebung und Rechtsprechung sowie dem „anerkannten Stand von Wissenschaft und Praxis" bzw. „Stand der Technik" („hard law") ausrichten. Auf der regulatorischen Seite ist Kenntnis der zwingenden Anforderungen aus diversen Quellen und Erfüllung durch angemessene Maßnahmen Pflicht.[2] Zahlreiche Einzelgesetze, (z.B. Produkthaftungsgesetze, KI-Verordnung, Umweltstrafrecht, ...), einschlägige öffentlich- und privat-rechtliche Regulierung, Straf- und Ordnungswid-

* Prof. Dr. Josef Scherer, Rechtsanwalt, Technische Hochschule Deggendorf.

1 Der Artikel lehnt sich an Scherer, KI-Verantwortung und enthaftende Wirkung eines KI-Compliance-Managementsystems, 2023, Risknet.de und Scherer/Grötsch/Fruth, Enthaftende Wirkung eines Compliance- und Hinweisgebersystems, 2023, Risknet.de, an; zu Technical Governance vgl. Scherer/Fruth, Technik-Governance, Sonderdruck des Bundesverbandes der Compliance-Manager, 1/2015.

2 Vgl. Scherer, Compliance-Managementsystem nach DIN ISO 37301: 2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 2022, Kapitel 4.5.

rigkeitenrecht, Rechtsprechung, u.v.m. beschäftigen sich mit sich z.T. überschneidenden, zwingend zu beachtenden Themen aus Nachhaltigkeit (ESG) und Governance (GRC) im Zusammenhang mit Innovationen, Produkten, sonstigen Leistungen und neuen Technologien.[3] Der technische Fortschritt führt zu ständig neuen Regulierungen, die es zu beachten gilt.

3. Beispiel: Entwurf der neuen EU-Produkthaftungsrichtlinie mit Bezug zu KI[4]

Das Produkthaftungsgesetz (ProdHaftG) statuiert eine Gefährdungshaftung, also eine verschuldensunabhängige Haftung des Herstellers. Die EU-Kommission hat im September 2022 den Entwurf für eine neue EU-Produkthaftungs-Richtlinie beschlossen. Am 14.12.2023 verständigten sich Unterhändler des Europaparlaments und der Mitgliedstaaten auf eine gemeinsame Position.

Auslöser war, dass in immer mehr Produkten Software und künftig auch KI-Komponenten enthalten sein werden. Während im Rahmen der deliktischen Produzentenhaftung nach § 823 BGB die vorherrschende Meinung annimmt, dass IT und Software (inkl. KI) auch von dieser Norm umfasst sei, war dies im Bereich des Produkthaftungsgesetzes noch umstritten.

Insofern erfolgt nun eine Klarstellung, dass IT und KI als Produkt im Sinne des ProdHaftG gelten soll. Die Länder der EU müssen nach Inkrafttreten der Richtlinie diese europäischen Vorgaben auch in ihre Produkthaftungsgesetze umsetzen.

Durch die Änderungen werden erhebliche neue Risiken im Zusammenhang mit Digitalisierung und KI auf Hersteller von Produkten, Importeure, Labeler, Bevollmächtigte des Herstellers im Sinne des Produktsicherheitsrechts und Fulfillment-Dienstleister (Art. 4 und 7 des Richtlinienentwurfs) zukommen. Diese Entwicklung beeinflusst damit die KI-Compliance und natürlich auch die Product Compliance einer Organisation.[5]

Die Produkthaftung in den zur EU gehörigen Ländern wird sich damit auch auf digitale Produktions-Dateien und Software erstrecken, wobei unter Software auch Systeme künstlicher Intelligenz fallen. Die Fehlerhaftigkeit im Sinne des Produkthaftungsgesetzes bezieht sich in erster Linie auf die Sicherheit, die durchschnittliche Kunden unter Berücksichtigung aller Umstände, auch naheliegender Fehlanwendungen, berechtigterweise erwarten dürfen. Damit sind künftig die Gefahren für Cyber-, IT-, Datenschutz-, Informations-Sicherheit und vieles mehr enthalten.

Der angemessene Sicherheitsstandard lässt sich nur aus einer angemessenen Risikobewertung ableiten. Selbst bei Billigprodukten ist eine Basis-Sicherheit unter Berücksichtigung der schwächsten Nutzergruppe zu gewährleisten.

Während früher ab Inverkehrbringen des Produktes bei zu diesem Zeitpunkt bestehender Sicherheit nach dem ProdHaftG eine rechtliche Zäsur eintrat, sieht die Richtlinie eine fortbestehende Haftung vor, wenn der Hersteller sein Produkt nach diesem Zeitpunkt beispielsweise durch Software-Updates kontrollieren kann. Auch Beweiserleichterungen für Geschädigte sind in der Richtlinie enthalten: Der Entwurf der Richtlinie sieht vor, dass in Produkthaftungsfällen ähnlich einer „Disclosure of Documents" künftig auch in den europäischen Ländern vom Hersteller die in seinem Besitz befindlichen Beweismittel wie Konstruktionsdokumentation oder Erkenntnisse aus Reklamationen oder Feldversuchen etc. herauszugeben sind und bei unvollständiger Herausgabe schon aus diesem Grund der Hersteller den Prozess verlieren könne.

Nach dem ProdHaftG bestand bisher keine Haftung, wenn das Produkt nur deshalb fehlerhaft war, weil sich die Regeln zum Stand der Technik in nicht absehbarer Weise geändert haben, nachdem das Produkt auf den Markt gebracht wurde. Dass bei dieser sehr jungen Technologie der KI nicht absehbar wäre, dass der „aktuelle Stand von Wissenschaft und Technik"[6] sich nach Inverkehrbringen noch ändern würde, ist kaum vorstellbar. Insbesondere reicht hier schon aus, wenn der Fehler aufgrund eines besseren Standes der Technik nach Inverkehrbringen durch ein Sicherheitssoftware-Update abgestellt werden kann. Insofern kommt auch der Bereitstellung von Sicherheitsupdates für Produkte über eine lange Zeit, mindestens bis zum Ende der längsten Verjährungsfrist, eine neue Bedeutung zu.[7]

III. Abzuleitende organisatorische Maßnahmen

Intern bedarf es aufgrund der Abstraktheit der diversen (künftigen) gesetzgeberischen Vorgaben, vieler „unbestimmter Rechtsbegriffe" und aktuell noch fehlender Standards gesonderter Richtlinien (Policies/Betriebsvereinbarungen/etc.)[8] und Aktivitäten in den relevanten Prozessabläufen zur Erfüllung dieser Anforderungen.

1. Integration des Product- oder Nachhaltigkeits-CMS in das allgemeine CMS

Durch Integration des Product- oder Nachhaltigkeits-CMS in das allgemeine Compliance- oder ESGRC-Managementsystem werden idR die beschriebenen Anforderungen umgesetzt und zugleich eine enthaftende Wirkung erzeugt.

Bzgl. eines allgemeinen Compliance-Managementsystems hat die ISO weltweit und das DIN für Deutschland die DIN ISO 37301:2021 (Compliance-Managementsystem) veröffentlicht. Insbesondere deren Normkapitel 4.5 (Compliance-Anforderungen) und 4.6 (Compliance-Risikoanalyse) eignen sich gut,

3 Scherer/Grötsch/Romeike Bavarian Journal of Applied Sciences, (BJAS), 2022, S. 16.
4 Depping/Pöhls, Zum Umgang mit dem Risiko der Produkthaftung und dessen Verschärfung, 12.4.2023.
5 VDMA, Leitfaden Product Compliance, 2023.
6 Bundesverfassungsgericht, Kalkar-Entscheidung, 1978 und Scherer/Fruth, „Technik-Governance", BCM-Sonderdruck.
7 Scherer/Ketelsen Bavarian Journal of Applied Sciences, (BJAS), 2022, S. 16–18 und ISO 37000:2021 (Governance of Organizations), 6.8 Daten und Entscheidungen.
8 Vgl. z.B. Richtlinien zur Nutzung von ChatGPT in Lehre und Forschung – eine Einschätzung der AIDAHO-Projektgruppe, Uni Hohenheim.

auch Innovational Product oder Nachhaltigkeits-Compliance-Anforderungen und -Risiken zu identifizieren, zu bewerten und risikobasiert zu steuern.

„Normtext DIN/ISO 37301:2021

4.5 Compliance-Verpflichtungen

Die Organisation muss systematisch ihre aus ihren Aktivitäten, Produkten und Dienstleistungen resultierenden Compliance-Verpflichtungen identifizieren und deren Auswirkung auf ihren Betrieb beurteilen.

Die Organisation muss über Prozesse verfügen, um:
a) neue und veränderte Compliance-Verpflichtungen zu identifizieren, um kontinuierlich Compliance sicherzustellen;

b) die Auswirkungen der identifizierten Änderungen zu bewerten und alle notwendigen Änderungen des Managements der Compliance-Verpflichtungen einzuführen.

Die Organisation muss dokumentierte Informationen ihrer Compliance-Verpflichtungen aufrechterhalten."

2. Identifikation der Verpflichtungen und deren Risiken

Die Identifikation muss sicherstellen, dass sämtliche einzuhaltende Product- oder Nachhaltigkeits-Compliance-Anforderungen, auch internationale, soweit relevant,[9] bekannt sind. Diese Vorgaben lassen sich in einem agilen und sich ständig weiterentwickelnden prozessbezogenen Rechtskataster abbilden.[10] Dabei ist sicherzustellen, dass alle derzeit geltenden und zukünftigen (neue und sich ändernde) Anforderungen erkannt und nachweisbar eingehalten werden, wenngleich dies eine komplexe Aufgabe darstellt.[11] Und auch hier gilt: Nichtwissen schützt vor Strafe nicht.

Zunächst müssen wohl viele der bereits identifizierten und ebenso auf Basis eines entsprechenden Prozesses fortlaufend neu zu identifizierenden Anforderungen in eine (nicht nur für Juristen und Techniker) verständliche Sprache „übersetzt" werden.[12] Dabei kommt es zu der Schwierigkeit, „unbestimmte Rechtsbegriffe"[13] anhand existierender Rechtsprechung, aber auch unter Heranziehung technischer Normen, auslegen zu müssen.

3. Implementierung von Aktivitäten zur Erfüllung der Anforderungen in die Prozesse

Wenn nun feststeht oder entschieden wurde, welche konkrete Anforderung (priorisiert) zu erfüllen ist, müssen noch Prozessschritte, Aktivitäts- und Kompetenzvermittlungs-Maßnahmen abgeleitet, in die Prozesse implementiert und zur Wirksamkeit gebracht werden, um sicherzustellen, dass die Anforderung messbar, revisionssicher und dokumentiert erfüllt wird/wurde. Dies gelingt mit führenden Workflows, Automation, digitalen Prozess-Zwillingen[14] und Unternehmenskultur, Awareness, Kompetenz (Wissen, Verstehen, Können und Wollen) sowie einem wirksamen „Lines of Defense"-Steuerungs- und Überwachungssystem.

Dabei kann es im Falle eines Rechtsstreits auch zu einer Beweislastumkehr bzw. sekundären Darlegungslast des Unternehmens kommen, so dass nachgewiesen werden muss, unter welchen Bedingungen und von wem Entscheidungen getroffen wurden.[15]

Um sicherzustellen, dass die benötigten Informationen vorliegen, eignet sich ein Digital Decision Management-Tool, das den Entscheidungsprozess mit (semi-)künstlicher Intelligenz unterstützt und zur gleichen Zeit getroffene Interpretationen und Definitionen von „unbestimmten Rechtsbegriffen" revisionssicher dokumentiert.[16]

a) Risikobasierter Ansatz

Als effektive und effiziente Vorgehensweise bewährt sich zunächst, funktional/aufbauorganisationsbezogen die Unternehmensbereiche oder (moderner) ablauforganisationsbezogen die Prozesse des Unternehmens zu definieren. Sodann sind diesen Bereichen bzw. Prozessen die dort relevanten Anforderungen aus Rechtsgebieten und auch sonstigen verpflichtenden Anforderungen (aus anderen Quellen) zuzuordnen. Dabei ist ein risikobasierter Ansatz zu wählen. Da es sehr schwierig ist, stets sämtliche Compliance-Verpflichtungen zu identifizieren und zu erfüllen, sollte auf Basis einer Compliance-Risiko-Analyse mit den risikobehaftetsten Verpflichtungen begonnen werden. „Risikobasiert" heißt in diesem Kontext aber nicht, dass weniger wichtige Verpflichtungen dauerhaft unbeachtet bleiben dürfen.

Dazu heißt es in der DIN ISO 37301:2021 im Kapitel A.4.5 – Compliance-Verpflichtungen:

Ein risikobasierter Ansatz sollte gewählt werden, d.h. Organisationen sollten mit der Identifizierung der wichtigsten Compliance-Verpflichtung, die für das Geschäft relevant ist, beginnen und sich anschließend auf alle anderen Compliance-Verpflichtungen konzentrieren (…).

9 Scherer/Butt/Reimertshofer DB 1998, 469.
10 Scherer/Fruth, Integriertes Compliance-Managementsystem mit GRC (4.0), 2. Aufl. 2017, S. 71.
11 Raum, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten in Hastenrath, Compliance-Kommunikation, 2017, S. 33.
12 Vgl. Scherer/Ketelsen Bavarian Journal of Applied Sciences 2022.
13 BVerfG 8.8.1978 – 2 BvL 8/77, NJW 1979, 359; Detterbeck, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 18. Aufl., 2020, S. 105 f. sowie Scherer/Ketelsen, Technical-Product Compliance Managementsystem, Bavarian Journal of Applied Sciences, 2022.
14 Scherer/Rieger, Der Digitale Prozess-Zwilling im Gesundheitswesen – auch als Beitrag zu Nachhaltigkeit (ESG, CSR), systemische Existenzsicherung (Resilienz) und Governance in Journal für Medizin- und Gesundheitsrecht, Ausgabe 2–2021 (zum kostenlosen Download auf scherer-grc.net/publikationen).
15 Beck Aktuell – Heute im Recht, Dieselklagen – Sekundäre Darlegungslast und Prognose über die Gesamtlaufleistung, 17.8.2021, https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-dieselklagen-sekundaere-darlegungslast-und-prognose-ueber-die-gesamtlaufleistung.
16 Scherer, Digital Decision Management – die Verknüpfung von Digitalisierung, Nachhaltigkeit und GRC mit Entscheidungsmanagement, Strategieentwicklung, Zielerreichung und Berichterstattung „Aligning GRC with S (Strateg) & P (Performance)", 25.11.2020, https://www.scherer-grc.net/publikationen/digital-decision-management; Taylor, Digital Decisioning: Using Decision Management to Deliver Business Impact from AI, 2. Aufl., 2019.

b) Risiko-Bewertung bzgl. verpflichtender Anforderungen:

Eine Nichteinhaltung der verpflichtenden Anforderungen kann je nach Ausmaß – z. B. bei Gefahr für Leib und Leben Dritter oder Umweltgefährdung – für die Organisation und die verantwortlichen Organe und/oder Mitarbeiter zu existenzvernichtender Wirkung, Freiheitsstrafen, Geldstrafen und Schadensersatzforderungen einschließlich Reputationsverlust führen.[17] Die Risiko-Bewertung hat auch für Product oder Nachhaltigkeits-Compliance-Risiken angemessen, also nach anerkanntem Stand von Wissenschaft und Praxis, zu erfolgen: Quantifizierung, Aggregation und die Betrachtung der Risikotragfähigkeit ist Standard.[18]

Zur Risiko-Steuerung ist es notwendig, die Ausrichtung und Compliance-Kultur des Unternehmens über regelmäßige Schulungen und den „Tone-from-the-Top" den Mitarbeitern kontinuierlich ins Bewusstsein zu rücken, damit diese stets im Sinne des CMS handeln.[19] Die Implementierung und Wirksamkeit von Aktivitäten zur Sicherstellung der Verpflichtungen in die Prozesse ist wesentlich effektiver als lediglich im Übermaß Richtlinien und dergleichen zu erlassen. Durch das „Lines-of-Defense"-Modell mit Compliance, Risikomanagement, IKS und Revision,[20] die Einrichtung von (KI-gestützten) Monitoring-Prozessen,[21] neutralen Ombudspersonen[22] und die Zertifizierung des Product CMS als Bestandteil eines integrierten Risiko- und Compliance-Managementsystems sollte die Überwachung und Reifegradbewertung des Compliance-Prozesses und der Komponenten des CMS gewährleistet werden. Dadurch werden auch Risiken der Abweichung von Vorgaben identifiziert und Aktivitäten zu Verbesserungen des Prozesses und der Komponenten abgeleitet.

c) Compliance-Verpflichtungen in jeder „Managementsystem-Insel" und jedem Standard

Bei einem Umwelt-Managementsystem (ISO 14001) muss für die Einhaltung umweltrechtlicher Anforderungen gesorgt werden, bei einem Informationssicherheits-Managementsystem (ISO/IEC 27001 ff.) sind es informationssicherheitsrechtliche Anforderungen. Beim Qualitäts-Managementsystem ist Product-Compliance ein zwingendes Thema. In der Praxis jedoch findet dies häufig mangels entsprechender Compliancemanagement-Kompetenzen nur wenig Beachtung. Die Früherkennung existenzgefährdender (Compliance-)Risiken ist auch gemäß § 1 StaRUG und § 91 Abs. 2 (und für börsennotierte Gesellschaften: Abs. 3 neu) AktG Pflicht.

IV. Enthaftende Wirkung eines Product- oder Nachhaltigkeits-Compliance-Managementsystems nach höchstrichterlicher Rechtsprechung[23]

1. Allgemeine, internationale Rechtsfigur und gefestigte Rechtslage in Deutschland: Enthaftende Wirkung einer Compliance-Organisation[24]

In jüngster Zeit bestätigten die höchstrichterliche deutsche und europäische Rechtsprechung (vgl. BGH-Entscheidungen „KMW", „Selbstreinigung", „Geschäftsverteilung" und EuGH-Entscheidungen „Deutsche Wohnen", „Hackerangriff" und „Umsatzsteuerbetrug")[25], Gesetzgeber[26] und Exekutive[27] die allgemein anzuerkennende Rechtsfigur, dass organisatorische Vorkehrungen zur Vermeidung von Pflichtverstößen unter Umständen im Einzelfall den Vorwurf vorsätzlichen Handelns entfallen lassen oder bei der Strafzumessung zu berücksichtigen sind. Auch der Gesetzesentwurf des Bundesjustizministeriums zur Unternehmenssanktion bei Compliance-Verstößen[28] ging in diese Richtung. Die Justizministerkonferenz der Länder bat im Mai 2023, einen neuen Entwurf für die aktuelle Legislaturperiode vorzulegen.

Ob die Implementierung bestimmter organisatorischer Mechanismen privilegierende Wirkung entfaltet, hängt vom Haftungsmodell der jeweiligen nationalen Rechtsordnung ab.[29] Das Konzept existiert in den USA seit den 1980er Jahren in Form der US Sentencing Guidelines. Internationale Standards verweisen ebenfalls auf diese Wirkungen.[30]

Dass Compliance-/Kontroll-Systeme tatbestandsausschließend oder bei der Strafzumessung positiv zu berücksichtigen sind, ist in Deutschland nunmehr gefestigte Rechtslage,[31] wenngleich bei Instanzgerichten, (Verfolgungs-)Behörden und auch in Wissenschaft und Praxis hierzu noch für Transparenz gesorgt werden muss.

17 BAG 29.4.2021 – 8 AZR 246/20, NJW 2021, 3483 und United States District Court for the District of Columbia, Consent Decree Civil Action Nos. 1:20-cv-2564, 1:20-cv-2565, 14.9.2020, S. 41 f., https://www.epa.gov/enforcement/daimler-ag-and-mercedes-benz-usa-llc-clean-air-act-civil-settlement-consent-decree.

18 Institut Deutscher Wirtschaftsprüfer, Prüfungsstandard 340:2020 und vgl. Scherer/Romeike/Gursky Journal für Medizin- und Gesundheitsrecht 2021, 159.

19 Scherer/Fruth, Governance-Management Band II (Standard & Audit), 2015, S. 130.

20 Ebenda, S. 188 f.

21 Noack, Künstliche Intelligenz und die Unternehmensleitung in Festschrift für Christine Windbichler zum 70. Geburtstag am 8. Dezember 2020, S. 956.

22 Scherer/Fruth, Governance-Management, Band I, 2015, S. 186.

23 Ausführlicher hierzu: Scherer/Grötsch/Fruth, Enthaftendes Compliance- und Whistleblowing-Managementsystem nach aktueller Rechtslage – Ein „Must have" für alle Führungskräfte!, Risknet, 2023.

24 Scherer, Compliance-Managementsystem nach DIN ISO 37301 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 2022, Herausgeber: DIN, S. 21 ff.

25 BGH 9.5.2017 – 1 StR 265/16, NJW 2017, 3798 (KMW), BGH 27.4.2022 – 5 StR 278/21, NStZ 2023, 35 (Selbstreinigung), BGH 9.11.2023 (Geschäftsverteilung), EuGH 5.12.2023 (Deutsche Wohnen),EuGH 14.12.2023 (Hackerangriff) und EuGH 24.1.2024 (Umsatzsteuerbetrug).

26 Vgl. § 38 Einführungsgesetz zur AO (EGAO), § 125 GWB.

27 Rundschreiben des Bundesministeriums für Finanzen (BMF) zu § 153 AO vom 23.5.2016, DStR 2016, 1218: „Tax Compliance" und die Pressemitteilung, vgl. Beyer, Bayern: Einbeziehung der Compliance in die Steuerprüfung, nwb.de vom 1.2.2023 des Bayerischen Ministeriums für Finanzen 2022 über die künftige Einbeziehung von Steuerkontrollsystemen in die steuerliche Prüfung.

28 Referentenentwurf: Gesetz zur Förderung der Unternehmensintegrität vom September 2020.

29 Trüg NZWiSt 2022, 106 f.

30 Vgl. Einleitung zur (DIN) ISO 37301:2021.

31 Trüg, Die Verteidigung von Unternehmen NZWiSt 2022, 106 f.

2. Ausgangslage: Die haftungsbewehrte Pflicht für Leitungs- und Aufsichtsorgane zur Einrichtung eines angemessenen und wirksamen Compliance-/Kontroll-Systems

Das Thema ist nicht nur für Konzerne, sondern auch für den Mittelstand höchst virulent.

Das OLG Nürnberg[32] stellte jüngst fest, dass die Pflicht zur Einrichtung eines angemessenen und wirksamen Internen Kontroll- und Compliance-Managementsystems (IKS) auch bereits für Geschäftsführer kleinerer Unternehmen gilt. Dies stellte im Siemens-Fall das Landgericht München („Neubürger") bereits 2013 fest. Gesetzlich vorgeschrieben ist ein Compliance-Managementsystem in bestimmten Branchen (vgl. §§ 29 VAG, 25a KWG) bzw. für alle „großen" Unternehmen (§ 91 AktG) seit Langem. Der Bundesfinanzhof[33] bekräftigte jüngst die ständige Rechtsprechung,[34] dass eine rechtskonforme (enthaftende) Pflichtendelegation auch die kontinuierliche Überwachung des Delegationsempfängers voraussetzt und Geschäftsführer ohne diese (Compliance-)Kompetenzen das Amt gar nicht antreten oder niederlegen sollten.

Sehr interessant ist auch bezüglich der Abgrenzung der Aufgaben des Leitungsorgans und der „ausdrücklich Beauftragten" (§§ 30, 9 Abs. 2 OWiG) ein aktuelles Urteil des Arbeitsgerichts Heilbronn:[35] Primär verantwortlich für die organisatorische Umsetzung von technischen und organisatorischen Maßnahmen (TOM) zur Herstellung eines angemessenen Datenschutzniveaus sei der Arbeitgeber und nicht der Datenschutzbeauftragte als „ausdrücklich Beauftragter", sofern diese Verantwortlichkeit nicht klar anders in der Beauftragung geregelt sei („ordnungsgemäße Übertragung von Unternehmerpflichten"). Darüber hinaus bräuchten Beschäftigte, die als (Datenschutz-) „ausdrücklich Beauftragte" benannt werden, ausreichend zeitliche Ressourcen, um ihrer Verantwortung gerecht zu werden. Angemessene (zeitliche) Ressourcen zur ordnungsgemäßen Wahrnehmung des Amtes stellten eine wesentliche Voraussetzung für eine ordnungsgemäße, enthaftende Übertragung von Unternehmerpflichten dar.

V. Haftung der Organisation, der Leitungs- und Aufsichtsorgane und der gemäß § 9 Abs. 2 OWiG ausdrücklich Beauftragten für eigene oder fremde schuldhafte Pflichtenverletzung

1. Haftung für eigene schuldhafte Pflichtverletzungen

Die Organisation haftet in der Regel nur, wenn ihr eine schuldhafte Pflichtverletzung ihrer Organe oder besonders Beauftragten zugerechnet werden kann (§§ 130, 30 OWiG, 84 DSGVO). Eine verschuldensunabhängige Haftung („Strict liability"/Gefährdungshaftung) der Organisation besteht in der Regel nicht.[36] Ein Unternehmensstraf- oder Unternehmenssanktionsrecht, wie in anderen Ländern oder in der letzten Koalition entworfen,[37] gibt es bisher in Deutschland nicht.

2. Haftung der Leitungsorgane und „ausdrücklich Beauftragter" bei eigenem, aktiven Tun

Sofern der schuldhafte Pflichtverstoß von Leitungsorgan oder „ausdrücklich Beauftragtem" selbst begangen wurde, haften diese nach allgemeinen Grundsätzen der Innen- und Außen-Haftung. Es erfolgt dann auch eine Zurechnung des schuldhaften Pflichtverstoßes an die Organisation. Auch Mitglieder des Aufsichtsorgans können wegen Verletzung ihrer Aufsichtspflichten, z.B. wegen eines fehlenden angemessenen und wirksamen Risiko-, Compliance-, Internen Kontroll-Systems, persönlich haften (§§ 116, 107 AktG).

3. Haftung der Leitungsorgane und „ausdrücklich Beauftragten" bei schuldhaften Pflichtverletzungen von Beschäftigten unterhalb der Leitungsebene

Eine schuldhafte Pflichtverletzung von Beschäftigten unterhalb der Leitungsebene kann zur eigenen schuldhaften Pflichtverletzung der Leitungsorgane oder „ausdrücklich Beauftragten" führen, wenn ein Mangel des Kontroll- und Überwachungs-Systems (mit-)ursächlich für den schuldhaften Pflichtverstoß der Beschäftigten war (mittelbare Verantwortung durch Aufsichtspflichtverletzung/Organisationspflichtverletzung). Diese Pflichtverletzung der Leitungsorgane oder „ausdrücklich Beauftragten" kann wiederum der Organisation haftungsbegründend zugerechnet werden. Auch die Mitglieder von Aufsichtsgremien können in diesen Fällen u.U. haften.

4. Enthaftende Wirkung auf Tatbestandsebene durch Einrichtung eines (Product- oder Nachhaltigkeits-)Compliance-/Kontroll-Systems

Das Leitungsorgan kann bei ordnungsgemäßer Pflichtendelegation und/oder Übertragung von Unternehmerpflichten auch Verantwortung auf „ausdrücklich Beauftragte" delegieren.

Primär- und Letzt-(Überwachungs-)Verantwortung bleibt in der Regel beim Leitungsorgan.

Die Einrichtung eines angemessenen und wirksamen Kontroll- und Überwachungs-Systems (ESGRC-, Compliance-, Tax-, Risiko-, IKS-, etc. Managementsystems) lässt bei Pflichtverletzungen durch Beschäftigte unterhalb der Leitungsebene i.d.R. die Pflichtverletzung durch Organisations- oder Überwachungsverschulden beim Leitungsorgan oder „ausdrücklich Beauftragten" bereits auf der Tatbestandsebene entfallen.[38] Dann kann auch keine Zurechnung einer schuldhaften Pflichtverletzung zulasten der Organisation/des Unternehmens zur Haftung (§§ 130, 30 OWiG, 84 DSGVO) derselben führen. Ebenso ist in diesen Fällen auch den Mitgliedern von Aufsichtsgremien kein Vorwurf zu machen.

32 OLG Nürnberg 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.
33 BFH 15.11.2022 – VII R 23/19, ZIP 2023, 1689.
34 Scherer, Business Partner Screening, 2017, gmrc.de, mit weiteren Nachweisen.
35 ArbG Heilbronn 29.9.2022 – 8 Ca 135/22, ZD 2023, 119.
36 EuGH 27.4.2023 – C 807/21, Schlussanträge des Generalanwalts.
37 Referentenentwurf zum Unternehmenssanktionsrecht („Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft") vom 16.6.2020.
38 Trüg NZWiSt 2022, 106 f.

Nach der Tat könnten Selbstanzeige,[39] „tätige Reue“ oder Kronzeugenregelungen (vgl. Kartellrecht) zur Befreiung von Sanktionen führen.

4. Berücksichtigung eines (Product- oder Nachhaltigkeits-)Compliance-Managementsystems, Hinweisgeber-Systems und eines „Selbstreinigungsprozesses“ nach der Tat im Straf- und Bußgeldverfahren bei Strafzumessung

Bei der Straf-/Bußgeldzumessung ist unter „Nachtatverhalten“[40] ein Selbstreinigungsprozess, die Einrichtung eines Compliance-Managementsystems und Hinweisgebersystems aufgrund wiederholt bestätigender Rechtsprechung des BGH zu berücksichtigen.[41]

Die Anforderungen, die die Rechtsprechung, unter anderem der BGH aus dem Jahr 2017 unter Verweis auf Raum, an ein enthaftend/strafmildernd wirkendes Compliance-Managementsystem und Hinweisgebersystem stellt, ergeben sich aus eben diesen Quellen im Zusammenwirken mit diversen aktuellen Standards für Compliance-Managementsysteme zum Beispiel DIN ISO 37301:2021, COSO I:2017 und IDW PS 980:2022.

Viele Organisationen haben bereits bemerkt, dass der Ansatz eines integrierten ESGRC-Managementsystems effektiver und zugleich wesentlich kostengünstiger ist, als zahllose „Insel-Systeme“ bürokratisch, mit hohen Kosten und wenig Wertbeitrag zu verwalten.

Entsprechend häufen sich Anfragen nach Kombi-Zertifikaten bei den Zertifizierenden. Erste Zertifizierungsstellen sind für Compliance-Managementsysteme nach ISO 37301 von der DAkkS[42] akkreditiert und bieten an, Product- oder Nachhaltigkeits-Compliance auch gesondert als fachlichen Scope eines CMS oder ESGRC-Managementsystems zu auditieren oder zu zertifizieren. Eine Zertifizierung ist auch in Kombination mit einem u.U. bereits bestehendem Qualitäts-Managementsystem möglich.[43]

39 Hauschka/Moosmayer/Lösler-Besch/Starck, Corporate Compliance, 3. Aufl. 2016, § 33 Tax Compliance, Rn. 81.

40 In älteren Prüfungsschemata findet die aktuelle Rechtslage häufig noch keine angemessene Berücksichtigung, vgl. z.B. Schäfer/Sander/Gemmeren, Praxis der Strafzumessung, 6. Aufl. 2017, Teil 4: Die strafzumessungserheblichen Umstände, Rn. 586.

41 Trüg NZWiSt 2022, 106.

42 Deutsche Akkreditierungsstelle GmbH.

43 Zur Vertiefung: Scherer, Compliance-Managementsystem nach DIN/ISO 37301 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 2022.